A P R I T Y

Aprity — Data Privacy & GDPR Compliance

Data Privacy Practices & GDPR Compliance

PUBLIC

Version 1.0 | March 2026 | aprity.ai

1. Executive Summary

Aprity is designed with privacy by design and by default. The platform analyzes **Salesforce metadata** (code, configuration, automation) — not business data or personal information. This document describes how Aprity handles data in compliance with the **General Data Protection Regulation (GDPR)**.

2. Data Controller vs. Data Processor

Role	Entity
Data Controller	The customer (your organization)
Data Processor	CRMIT (Aprity platform operator)

Aprity processes data on behalf of the customer, following their instructions (scan initiation, configuration). A **Data Processing Agreement (DPA)** is available upon request.

3. What Data is Processed?

3.1 Salesforce Metadata (Non-Personal Data)

Data Type	Examples	Personal Data?
Code	Apex classes, triggers, test classes	No
Automation	Flows, Workflow Rules, Process Builders	No
Schema	Object names, field names, record types	No
Security config	Permission sets, profiles, sharing rules	No
Validation	Validation rules, formula fields	No

> ***Important**: Salesforce field *names* (e.g., "Email__c", "Phone__c") are metadata describing the schema structure. Aprity never reads the *values* stored in these fields.*

3.2 Technical Data (Limited Personal Data)

Data Type	Purpose	Retention	Legal Basis
Salesforce admin username	JWT authentication	Duration of service	Legitimate interest
Salesforce org ID	Tenant identification	Duration of service	Contract performance
IP addresses (logs)	Security monitoring	90 days	Legitimate interest

Admin console user accounts	Platform administration	Duration of service	Contract performance

3.3 Data Never Processed

Category	Guarantee
Salesforce business records	Never accessed via Metadata API
End-user PII	Not collected, stored, or transmitted
Cookies / tracking	No user tracking on the platform
Biometric data	Not applicable

4. Data Residency & Transfers

Component	Location	Provider
Application hosting	**Azure France Central** (Paris)	Microsoft Azure
Database (Cosmos DB)	**Azure France Central**	Microsoft Azure
File storage (Blob)	**Azure France Central**	Microsoft Azure
Secret vault (Key Vault)	**Azure France Central**	Microsoft Azure
AI processing	Configurable (see Section 7)	Configurable

4.1 International Transfers

- **Default configuration**: All data remains in the EU (France Central region)
- **AI providers**: When using Anthropic Claude or OpenAI, prompts may be processed outside the EU. Customers can mitigate this by:
  - Using **Azure OpenAI** (data stays in the chosen Azure region)
  - Using a **BYO-LLM** endpoint hosted in the EU
  - Configuring a provider that offers EU data residency

> *All transfers are governed by Standard Contractual Clauses (SCCs) where applicable.*

5. Data Retention & Deletion

5.1 Automatic Retention Policies

Data Type	Retention	Mechanism
AI interaction logs	30 days	Automatic TTL (Time-to-Live)

Authentication nonces	1 hour	Automatic TTL
OAuth session states	10-30 minutes	Automatic TTL
Activation codes	30 days	Automatic TTL

5.2 Persistent Data

Data Type	Retention	Deletion
Generated documentation	Until customer requests deletion	On request
Scan history & events	Until customer requests deletion	On request
Metadata analysis cache	Until next scan or deletion request	On request
Connection configuration	Until customer requests deletion	On request

5.3 Right to Erasure (Article 17)

Customers can request complete deletion of their data:

1. **Scope**: All tenant data, scan results, documentation, configuration
2. **Timeline**: Within 30 days of validated request
3. **Method**: Administrative request to support@aprity.ai
4. **Confirmation**: Written confirmation of deletion provided

6. Data Subject Rights (GDPR Articles 15-22)

Right	Applicability	How to Exercise
Access (Art. 15)	Limited — minimal personal data processed	Contact DPO
Rectification (Art. 16)	Connection metadata (username, org ID)	Admin console or support
Erasure (Art. 17)	Full tenant data deletion	Support request
Portability (Art. 20)	Documentation export (Markdown, HTML, DOCX)	Self-service via platform
Restriction (Art. 18)	Scan suspension	Admin console
Objection (Art. 21)	Service termination	Contract termination

7. AI Processing & Sub-Processors

7.1 Sub-Processors

Sub-Processor	Purpose	Location	Data Shared
Microsoft Azure	Cloud infrastructure	France Central (EU)	All platform data
Anthropic (Claude)	AI analysis (default)	US	Salesforce metadata only
OpenAI	AI analysis (optional)	US / EU (Azure)	Salesforce metadata only
Atlassian	Confluence export (optional)	Regional	Generated documentation

7.2 BYO-LLM Option

Enterprise customers can configure their own AI endpoint:

- **Azure OpenAI**: Data stays in your chosen Azure region
- **Self-hosted models**: Full control over AI processing location
- **Custom endpoints**: Any OpenAI-compatible API

> *This eliminates international data transfers for AI processing.*

7.3 AI Data Handling

Aspect	Policy
Data sent to AI	Metadata only (code, schema, config names)
Business data sent	Never
AI training on your data	No (zero-retention API agreements with providers)
Audit trail	Every AI interaction logged for 30 days

8. Security Measures (Article 32)

Measure	Implementation
Encryption in transit	TLS 1.2+ (all communications)
Encryption at rest	AES-256 (Azure platform)
Access control	HMAC-SHA256 authentication, role-based admin
Tenant isolation	Database-level partition keys
Secret management	Azure Key Vault (HSM-backed)
Audit logging	Immutable logs with tenant context
Breach detection	Azure Application Insights monitoring

9. Data Protection Impact Assessment (DPIA)

Given that Aprity:

- Does **not** process personal data at scale
- Does **not** perform profiling or automated decision-making
- Does **not** process special categories of data (Article 9)
- Processes only **metadata** (structural, not content)

A formal DPIA is generally **not required**. However, customers may conduct their own assessment, and Aprity will provide all necessary information to support it.

10. Breach Notification (Articles 33-34)

In the event of a personal data breach:

Step	Timeline
Internal detection & assessment	Within 24 hours
Notification to affected customers	Within 72 hours
Notification to supervisory authority (if required)	Within 72 hours
Detailed incident report	Within 30 days

11. Data Processing Agreement (DPA)

A standard DPA is available covering:

- Subject matter and duration of processing
- Nature and purpose of processing
- Type of personal data and categories of data subjects
- Obligations and rights of the controller
- Sub-processor management
- International transfer safeguards
- Audit rights

To request a DPA: contact legal@aprity.ai

Contact

Role	Contact
Data Protection Officer	dpo@aprity.ai
Security Team	security@aprity.ai
Legal	legal@aprity.ai

This document describes Aprity's data privacy practices as of March 2026. For the most current information, please contact our DPO.